

**Statement of Work**  
**Autonomous Mobile Delivery Robot**  
**NIH-CC-18-013336**

Table of Contents

<b>PART 1 – GENERAL INFORMATION .....</b>	<b>3</b>
<b>PART 3 - GOVERNMENT FURNISHED PROPERTY, EQUIPMENT, AND SERVICES.....</b>	<b>8</b>
<b>PART 4 - CONTRACTOR FURNISHED ITEMS AND SERVICES .....</b>	<b>9</b>
<b>PART 5 – OTHER SYSTEM AND TECHNICAL SPECIFICATIONS.....</b>	<b>10</b>
<b>PART 6 – PROJECT MANAGEMENT, IMPLEMENTATION, SERVICE.....</b>	<b>15</b>
<b>PART 7 - APPLICABLE PUBLICATIONS .....</b>	<b>18</b>
<b>PART 8 - DEFINITIONS &amp; ACRONYMS .....</b>	<b>19</b>
<b>Technical Exhibit 1 – Deliverables Schedule (Upon Request by COR).....</b>	<b>20</b>
<b>Technical Exhibit 2 – Estimated Workload Data (Upon Request by COR).....</b>	<b>21</b>
<b>Technical Exhibit 3 – CC Data Center.....</b>	<b>22</b>
<b>Technical Exhibit 4 – CC Remote Access Options.....</b>	<b>23</b>

**SOW: Autonomous Mobile Delivery Robot**

**PART 1 – GENERAL INFORMATION**

The Clinical Center (CC) Pharmacy employs approximately 45 staff inpatient and outpatient pharmacists and approximately 35 staff inpatient and outpatient pharmacy technicians. The inpatient section is further divided into Unit Dose (UD) and Intravenous Admixture Unit (IVAU). The pharmacy is open 24 hours a day, seven days a week. Pharmacists and pharmacy technicians cover approximately 30 or more different shifts during this time period. The Unit Dose section of the Pharmacy Department dispenses, on average, 40,000 unit dose medications per month. The IVAU is responsible for the compounding of sterile injectable preparations.

The purpose of this acquisition is to acquire an autonomous mobile delivery robot system to deliver pharmaceuticals throughout the NIH Clinical Center.

This Statement of Work (SOW) issued by National Institute of Health, Clinical Center describes the goals expected to be achieved with regard to planning, delivery, installation and support.

**1.1 Introduction**

The National Institutes of Health (NIH), a part of the U.S. Department of Health and Human Services, is the primary federal agency for conducting and supporting medical research. Helping to lead the way toward important medical discoveries that improve people's health and save lives, NIH scientists investigate ways to prevent disease as well as the causes, treatments, and even cures for common and rare diseases. Composed of 27 institute and centers, the NIH provides leadership and financial support to researches in all fifty states and throughout the world.

The Clinical Center at the NIH in Bethesda, Maryland, is the nation's largest hospital devoted to clinical research. It is a national resource that makes it possible to rapidly translate scientific observations and laboratory discoveries into new approaches for diagnosing, treating, and preventing disease. Approximately 1,500 studies are in progress at the NIH Clinical Center. About half the studies are the first tests of new medications or medical treatments in patients

**1.2 Current Environment:**

The Department of Pharmacy's primary operating objective is to support and conduct research by providing safe, high quality care – one patient – one medication at a time. The secondary operating objective is standardize, improve effectiveness (service, outcomes), and reduce waste.

**1.3 Objectives:**

To purchase and install an autonomous mobile delivery robot system that can be used across the entire clinical center.

**SOW: Autonomous Mobile Delivery Robot**

**1.4 Scope of Work**

The contractor shall provide hardware, software, services, and up to 2 mobile robots, to be used by the Pharmacy Department. Additional robots up to 10 may be desired.

- 1.4.1** The Contractor shall provide a non-developmental autonomous mobile medication delivery robot that will operate as a single integrated solution. The solution shall be commercial off the shelf software and hardware components that are configurable to the NIH Clinical Center workflow. The solution must have been demonstrated and proven to be in use at another inpatient hospital setting.
- 1.4.2** The robot shall be fully autonomous without tracks or cables.
- 1.4.3** The robot shall be capable of detecting and maneuvering around an obstacle in its designated path.
  - 1.4.3.1** Able to move laterally in order to bypass an obstruction before returning to the set route.
  - 1.4.3.2** Can rotate in place to quickly change direction while requiring less space.
- 1.4.4** The robot shall be able to autonomously navigate NIH CC using sensors to safely detect surrounding objects and persons.
- 1.4.5** The system shall have multiple dispatch nodes such as scheduled, touchscreen monitor and handheld ad-hoc requests.
- 1.4.6** The robot must have at least 8 hours of battery run time with intermittent charging.
  - 1.4.6.1** Battery life must be sufficient enough to last for multiple trips in succession without the need for a recharge.
  - 1.4.6.2** A full recharge of the autonomous robot should take at maximum five hours.
  - 1.4.6.3** The system shall be able to charge while requiring little to no modification of the current wall outlet charging station using a docking station. A normal 110 volt wall outlet is preferred to recharge batteries.
- 1.4.7** The robot shall be able to transition to carpet smoothly.
- 1.4.8** The system shall securely transport medications to/from locations throughout the hospital.
- 1.4.9** The robot shall have locked drawers that require biometrics and/or unique PIN to access medications and supplies transported.
- 1.4.10** The system shall have flexible configurations to accommodate the delivery needs for all services requesting use of the mobile robot.
- 1.4.11** The robot shall deliver contents timely and safely.
- 1.4.12** The autonomous robot shall use a navigation system that can be easily reconfigured during construction and temporary closures in the hospital.
- 1.4.13** The robot shall have the ability to navigate through secured doors and elevators.
- 1.4.14** The robot shall have the ability to tow at least 500 pounds.
- 1.4.15** The robot shall have a software that will allow nursing and other staff members to remotely determine location of robot.
- 1.4.16** The system shall have a customizable reporting system.
- 1.4.17** The robot shall not endanger those nearby and should be able to stop in less than 2 feet when required.
- 1.4.18** The robot shall not easily tip over beyond 10 degrees in any direction.
- 1.4.19** The system shall be capable of using NIH-CC Wi-Fi network that is solely used for medical equipment.
- 1.4.20** The vendor shall provide customer support with remote virtual private network (VPN) ability and onsite repairs available 24 hours per day/7 days per week.

**SOW: Autonomous Mobile Delivery Robot****1.5 Contract Type and Period of Performance**

A single Firm Fixed Price type contract is contemplated for one 12-month base period and four 12-month option periods to extend the effective period of performance. Options to increase quantities may be exercised by formal modification to the contract should there be a need to provide additional equipment as the Department of Pharmacy Area expands.

The Period of Performance is estimated to begin sometime in August 2018 and run through August, 2023.

Estimated Periods of Performance is as follows.

Base Period: 8/1/2018 – 7/31/2019

Option Period One (1): 9/1/2019 - 8/30/2020

Option Period Two (2): 9/1/2020 - 8/30/2021

Option Period Three (3): 9/1/2021 - 8/30/2022

Option Period Four (4): 9/1/2022 - 8/30/2023

**1.6 Recognized Holidays:** Work may occur on Federal Holidays. Maintenance Support may occur all hours and across all days.

The ten holidays observed by the Federal Government are as follows:

New Year's Day	Memorial Day	Columbus Day	Christmas Day
Martin Luther King Day	Independence Day	Veterans Day	
President's Day	Labor Day	Thanksgiving Day	

Also, any other day declared by the President of the United States to be a National or Federal holiday.

**1.7 Hours of Operation:** The NIH CC operates 365 days per year, 24 hours per day including all holidays. Maintenance Support must be provided across all days and hours (365x24x7).

**1.8 Installation Timing:** The Contractor will work with the autonomous mobile medication delivery robot Implementation Team to schedule and perform the installation. Installation will be performed at the convenience of the location receiving the system. Installation may occur between the hours of 9:00 a.m. and 7:00 p.m., Monday through Sunday, including holidays and any day declared an official Federal Holiday.

**1.9 Place of Performance:** The work to be performed under this contract will be performed at the NIH Clinical Center Department of Pharmacy, 9000 Rockville Pike, Building 10, Bethesda MD 20892.

**1.10 Security Requirements:** Contractor personnel performing work under this contract must have a NIH CC Contractor badge which will require fingerprinting and a background check.

- a. **Physical Security:** The Contractor shall be responsible for safeguarding all government equipment, information and property provided for contractor use. At the close of each work period, government facilities, equipment, and materials shall be secured.
- b. **Key Control:** The Contractor shall establish and implement methods of making sure all keys/key cards issued to the Contractor by the Government are not lost or misplaced and are not used by unauthorized persons. NOTE: All references to keys include key cards. No keys issued to the Contractor by the Government shall be duplicated. The Contractor shall develop procedures covering key control that shall be included in the Quality Control Plan. Such procedures shall

**SOW: Autonomous Mobile Delivery Robot**

include turn-in of any issued keys by personnel who no longer require access to locked areas. The Contractor shall immediately report any occurrences of lost or duplicate keys/key cards to the NIH CC Contracting Officer.

1. In the event keys, other than master keys, are lost or duplicated, the Contractor shall, upon direction of the NIH CC Contracting Officer, re-key or replace the affected lock or locks; however, the Government, at its option, may replace the affected lock or locks or perform re-keying. When the replacement of locks or re-keying is performed by the Government, the total cost of re-keying or the replacement of the lock or locks shall be deducted from the monthly payment due the Contractor. In the event a master key is lost or duplicated, all locks and keys for that system shall be replaced by the Government and the total cost deducted from the monthly payment due the Contractor.
2. The Contractor shall prohibit the use of Government issued keys/key cards by any persons other than the Contractor's employees. The Contractor shall prohibit the opening of locked areas by Contractor employees to permit entrance of persons other than Contractor employees engaged in the performance of assigned work in those areas, or personnel authorized entrance by the NIH CC Contracting Officer.

**1.11 Special Qualifications:** The Contractor must ensure that all staff maintain his/her NIH badge which requires completion of annual training (i.e., security, privacy, first safety, Joint Commission).

**1.12 Post Award Conference/Periodic Progress Meetings:** The Contractor agrees to attend any post award conference convened by the contracting activity or contract administration office in accordance with Federal Acquisition Regulation Subpart 42.5. The NIH CC Contracting Officer, NIH CC Contracting Officers Representative (COR), and other Government personnel, as appropriate, may meet periodically with the contractor to review the contractor's performance. At these meetings, the NIH CC Contracting Officer will apprise the contractor of how the government views the contractor's performance and the contractor will apprise the Government of problems, if any, being experienced. Appropriate action shall be taken to resolve outstanding issues. These meetings shall be at no additional cost to the government.

**1.13 NIH CC Contracting Officer's Representative:** The NIH CC COR is a specialist from the NIH CC Pharmacy Department whose role is to define, plan, track and manage the project.

The following individual is designated as the NIH CC COR:

**Project Officer**

Name: TBD

Address: 10 Center Drive, Building #10, Room 1C240. Bethesda, MD 20850

Email: TBD

Phone Number: TBD

**1.14 NIH CC Implementation Team:** The NIH Technical Implementation Team includes the COR, Pharmacy Project Manager, Pharmacy Management, NIH CC IT staff, NIH CC Security staff.

**1.15 Executive Management Oversight:** Executive Management oversight for this project is provided by the NIH CC Chief Pharmacy and the NIH CIO.

**1.16 Identification of Contractor Employees:** All contract personnel attending meetings, answering Government telephones, and working in other situations where their contractor status is not obvious to third parties are required to identify themselves as such to avoid creating an impression in the minds of members of the public that they are Government officials. They must also ensure that all documents or reports produced by contractors are suitably marked as contractor products or that contractor participation is appropriately disclosed. Badges must be worn at all times.

**1.17 Data Rights:** The Government has unlimited rights to all documents/materials produced under this contract. All documents and materials, to include the source codes of any software, produced under this contract shall be Government owned and are the property of the Government with all rights and privileges of

**SOW: Autonomous Mobile Delivery Robot**

ownership/copyright belonging exclusively to the Government. These documents and materials may not be used or sold by the contractor without written permission from the NIH CC Contracting Officer. All materials supplied to the Government shall be the sole property of the Government and may not be used for any other purpose. This right does not abrogate any other Government rights.

**1.18 Organizational Conflict of Interest:** Contractor and subcontractor personnel performing work under this contract may receive, have access to or participate in the development of proprietary or source selection information (e.g., cost or pricing information, budget information or analyses, specifications or work statements, etc.) or perform evaluation services which may create a current or subsequent Organizational Conflict of Interests (OCI) as defined in FAR Subpart 9.5. The Contractor shall notify the NIH CC Contracting Officer immediately whenever it becomes aware that such access or participation may result in any actual or potential OCI and shall promptly submit a plan to the NIH CC Contracting Officer to avoid or mitigate any such OCI. The Contractor's mitigation plan will be determined to be acceptable solely at the discretion of the NIH CC Contracting Officer and in the event the NIH CC Contracting Officer unilaterally determines that any such OCI cannot be satisfactorily avoided or mitigated, the NIH CC Contracting Officer may affect other remedies as he or she deems necessary, including prohibiting the Contractor from participation in subsequent contracted requirements which may be affected by the OCI.

**1.19 Phase Out Period:** To reduce any decreases in productivity and to prevent possible negative impacts on additional services, the Contractor shall have personnel on board for 60 days prior to the contract phase out period. During the phase out period, the Contractor shall transfer any system knowledge to the Government.

**PART 3 - GOVERNMENT FURNISHED PROPERTY, EQUIPMENT, AND SERVICES**

**3. GOVERNMENT FURNISHED ITEMS AND SERVICES:**

The government will be responsible for:

- A.** Rack Space in NIH CC Data Center.
  - 1. Support Operating System of any Required Server.
  - 2. Provide Virtual Server(s) if the system can be virtualized.
  - 3. Perform Monthly OS Patches.
  - 4. Provide 2012 or greater MS SQL Server Enterprise License. Any and all databases must be encrypted.
- B.** Server Maintenance (See section 5)
  - 1. NIH CC DCRI will manage the OS, Patches, MS SQL 2012 Database or greater for the Physical Computer.

**SOW: Autonomous Mobile Delivery Robot**

**PART 4 - CONTRACTOR FURNISHED ITEMS AND SERVICES**

**4. CONTRACTOR FURNISHED ITEMS AND RESPONSIBILITIES:**

**The Contractor shall provide:**

- A.** Two initial autonomous robots with ability to add on up to 10 total robots.
- B.** Servers if the system cannot be virtualized.
- C.** All the software required to operate and manage the robotic delivery system.
- D.** Master list of all hardware and software components including length of warranty and average life of the solution. See Table 8.3.
- E.** Master list of Software Maintenance Agreements and License Agreements for all software.
- F.** All parking in accordance with NIH requirements.
- G.** Specifications required of the virtualized server, if applicable.

## PART 5 – OTHER SYSTEM AND TECHNICAL SPECIFICATIONS

- 5.1 Authentication:** The solution shall support integration with NIH directory services supporting an integrated authentication and authorization model (single sign on) utilizing the e-Government profile for Security Assertion Markup Language 2.0 (SAML 2.0).
- 5.2 Confidentiality, Security, and Privacy:** All patient data shall be stored on the server hosted on the premises at the National Institute of Health, Clinical Center. Responder personnel shall adhere to the Privacy Act, Title 5 of the U.S. Code, Section 552a and applicable agency rules and regulations. The Contractor will work with NIH CC Security Team for all FISMA/SAA documentation.
- 5.3 Construction and Wiring of the Solution**
- 5.3.1** All wiring between the camera and any other vendor hardware shall abide by the existing NIH/CIT Cable Standards and Guidelines (<http://orf.od.nih.gov/PoliciesAndGuidelines/BiomedicalandAnimalResearchFacilitiesDesignPoliciesandGuidelines/Pages/DesignRequirementsManualPDF.aspx> ) . This also includes any new infrastructure that is required for this installation.
  - 5.3.2** The Contractor is responsible for reviewing the plans for construction and wiring and must receive approval from the NIH CC COR before any work starts on an area by area basis.
  - 5.3.3** The Contractor must utilize existing pathways (i.e. conduits, cable tray) before installing new pathways between existing individual rooms or between any of the system components.
  - 5.3.4** The Contractor is responsible to ensure that all accountable government property, i.e. computer, computer displays, and servers, shall be delivered to the pharmacy procurement office at NIH Building 10 Room 1C-166
  - 5.3.5** The Contractor shall report all discrepancies noted that are not within the scope of this agreement to the NIH CC COR and the NIH CC Contracting Officer.
  - 5.3.6** The Contractor is responsible to get any repair or replacement of components not within the scope of this agreement, which will result in additional cost approved by the NIH CC Contracting Officer prior to procurement of the component and installation.
  - 5.3.7** NIH ORF policies and guidelines for pathway and infrastructure requirements must be followed and can be found at:  
<http://orf.od.nih.gov/PoliciesAndGuidelines/BiomedicalandAnimalResearchFacilitiesDesignPoliciesandGuidelines/Pages/DesignRequirementsManualPDF.aspx>
- 5.4 Server Specifications.** These requirements are for any workstation or hardware provided to support the autonomous robot if applicable.
- 5.4.1** The Contractor shall provide detailed specifications for installation and configuration of all hardware components including virtualization, web services and database requirements. Actual installation and configuration of servers in government furnished computer racks will be performed by Contractor.
  - 5.4.2** The Contractor will identify any and all licensing requirements for hardware, software, number of users, number of concurrent users, etc.
  - 5.4.3** The Server/Database/Application Infrastructure must be supported to run on Windows Server 2012 R2, at a minimum. Windows Server 2016 is preferred but a plan to migrate to Windows Server 2016 within one year is acceptable.

**SOW: Autonomous Mobile Delivery Robot**

- 5.4.4 The Server/Database/Application Infrastructure shall be updated monthly for security patches for vulnerabilities identified as critical, high or medium.
- 5.4.5 The Server/Application Infrastructure shall provide comprehensive tools for managing both client and server software configurations that minimize hands-on involvement of DCRI technical staff.
- 5.4.6 The Server/Application Infrastructure shall provide comprehensive security and confidentiality features including, but not limited to, biometric, password suppression, audit capabilities required by HIPAA, FISMA, and the Privacy Act, and ability to restrict or require data fields.
- 5.4.7 The Server/Application Infrastructure shall include redundancy for any servers required for the system. Servers should be configured in a high availability configuration and be clustered. Servers can be setup as virtual in the NIH CC Virtual Environment.
- 5.4.8 The Server/Application Infrastructure shall support FIPS 140-2 validated encryption at rest for all servers to support the Integrated System. This includes file systems and databases.
- 5.4.9 The Server/Application Infrastructure may support virtual servers on VMWare vSphere 6 as part of the NIH CC Virtual Environment.
- 5.4.10 The Server/Application Infrastructure configuration of hardware will comply with NIH standards for security hardening and install the NIH toolset of required applications, which will be performed by NIH.
- 5.4.11 The Server/Application Infrastructure will require multiple agents on each Server. These agents include but are not limited to: McAfee VirusScan 8.8 (Patch 8), FireEye, ForeScout, CA Asset Management Agent, CylancePROTECT Agent, Nagios, Nessus Agent, VMWare Tools (virtual only), NetBackup Agent (physical only), EMC PowerPath (physical, SAN connected hosts only).
- 5.4.12 The Server/Application Infrastructure shall provide end-to-end data in transit encryption (if web based the system must use SSL and be located behind the CC DMZ). The Server/Application Infrastructure shall provide data encryption of data at rest at both the hardware (physical) and file level.
- 5.4.13 The Server/Application Infrastructure shall provide tools for notifying system administrators in the event of slowness.
- 5.4.14 The Server/Application Infrastructure shall provide tools for notifying system administrators in the event of system down.
- 5.4.15 The Server/Application Infrastructure shall provide the ability to monitor and record data storage device usage.
- 5.4.16 The Server/Application Infrastructure shall provide tools for automated updating of client software.
- 5.4.17 The Server/Database Management System (RDBMS) Infrastructure must be MicroSoft (MS) SQL 2012 or greater. MS SQL 2014 is preferred.
- 5.4.18 The Server/Application/RDBMS must only utilize supported products. Unsupported hardware, software, operation systems, applications and database management system versions must be replaced one (1) year prior to end of life.
- 5.4.19 The Server/RDBMS Infrastructure configuration shall support mirroring with at least two nodes with the always on feature turned on.

**SOW: Autonomous Mobile Delivery Robot**

- 5.4.20 The Server/RDBMS Infrastructure configuration shall support encryption with HHS Standard for Encryption of Computing Devices and Information. All encryption solutions used throughout the Department and referenced throughout this document must be Federal Information Processing Standard (FIPS) 140-2 validated.
- 5.4.21 The Server/RDBMS Infrastructure shall support both complete and incremental backup of database and system files. Backups shall be able to be performed with the system up or down and shall not require taking the system down.
- 5.4.22 The Server/RDBMS Infrastructure shall provide the capability for exporting of system files to allow system restore capabilities.
- 5.4.23 The Server/RDBMS Infrastructure shall provide a fail over capability so that the application will resume operations in the event of server failure.
- 5.4.24 The Server/RDBMS Infrastructure failover capabilities will not require human intervention.
- 5.4.25 The Server/RDBMS Infrastructure failover procedures will not require changes in client configuration such as server TCP/IP addresses.
- 5.4.26 The Server/RDBMS Infrastructure shall provide the ability to recover the database from backups and transaction logs.
- 5.4.27 The Server/RDBMS Infrastructure shall provide tools for monitoring and enhancing system performance and load distribution across servers.
- 5.4.28 The Server/Application/RDBMS Infrastructure shall provide tools for automated setup of client software so that software can be installed without Information Technology staff involvement at each client workstation.
- 5.4.29 The Server/Application/RDBMS Infrastructure shall provide version control for server software.
- 5.4.30 The Server/Application/RDBMS Infrastructure shall provide version control for structure changes in the database

**5.5 Application Specifications.** These requirements are for any application that is accessible via NIH Workstations such as System Configuration, System Administration, end user dashboard, etc.

- 5.5.1 Applications shall have a consistent look and feel across modules and functions.
- 5.5.2 Applications shall be designed to utilize at least 1024x768 resolution when applicable.
- 5.5.3 Any application administration module that will require a full client must be provided via CITRIX XenApp 6.5 (current) and 7.12 (planned).
- 5.5.4 Applications shall work across Windows 7, 8, 10, Mac OS platforms and CITRIX to include 32-bit and 64-bit platforms.
- 5.5.5 Applications shall support the following browsers: MS IE 11 and greater, MS Edge; Google Chrome, Safari 9 and most current for MAC; and FireFox with the most current of each Internet Browser within 3 months of release
- 5.5.6 Applications shall not be dependent on browser specific controls.
- 5.5.7 Applications shall allow CC Administrators to set time-out duration based on organizational policy.
- 5.5.8 Applications shall provide the capability to exit with one keystroke or mouse-click after appropriate warnings have been acknowledged.
- 5.5.9 Applications shall provide a help file index.

**SOW: Autonomous Mobile Delivery Robot**

- 5.5.10** Applications shall provide the ability for NIH to customize electronic help files.
- 5.5.11** All points of login into the application should allow a customizable warning banner. This includes websites, mobile and desktop applications/software.
- 5.5.12** The Server/Application Infrastructure shall provide end-to-end data in transit encryption (if web based the system must use SSL and be located behind the CC DMZ).
- 5.5.13** The Server/Application Infrastructure shall provide data encryption of data at rest at both the hardware (physical) and file level.

**5.6 NIH Network Security/User Access Requirements.**

- 5.6.1** The web application shall require NIH Single Sign On/Active Directory for access.
- 5.6.2** The System shall provide the capability to automatically log users off after a specified period of inactivity using parameters that can be set by the system administrator.
- 5.6.3** The System shall provide restricted access to functions based upon user class.
- 5.6.4** The System shall always display the current user name.
- 5.6.5** The System shall require ID & non-displaying password.
- 5.6.6** The System shall have an access model that accommodates a variety of secure access methods, including, but not limited to, biometric or token-based access, and different access procedures for devices located inside the NIH intranet).
- 5.6.7** The System shall monitor multiple failed attempts to logon by triggering a system alert.
- 5.6.8** The System shall monitor multiple (i.e., 3) failed attempts to logon by disabling the login id.
- 5.6.9** The System shall connect/link/access with NIH active directory or NED Database to load all eligible employees into the system initially and to maintain the user list as employees come on board and leave.
- 5.6.10** The System shall allow CC staff to assign privileges to individual users of the system.
- 5.6.11** The System shall provide the ability to set up and manage user access and privileges using role-based security. Security Roles, at a minimum,
- 5.6.12** The System shall allow CC staff to assign security rights, with the possibility of further customization based on individual need, to assign a group of privileges to any user based on their role or on organizational need.
- 5.6.13** The System shall provide the ability to assign/restrict rights/privileges to the security roles. Security Rights, at a minimum,
  - A.** ability to add new users to the system
  - B.** ability to change users' roles and privileges
  - C.** ability to create reports, data analytic dashboards
  - D.** ability to run specific reports
  - E.** ability to view specific data analytic dashboards
  - F.** ability configure reports and dashboards and assign to specific roles
  - G.** Ability to configure pathways, screens, choice lists selections.
- 5.6.14** The System shall log user sessions.
- 5.6.15** The System shall maintain an audit capability that will log access or modification of individual patient records viewed on reports.
- 5.6.16** The System shall log system events (i.e., add an event, issue a report request).
- 5.6.17** The System event field displays shall include event date and time.

**SOW: Autonomous Mobile Delivery Robot**

**5.8.19** If the System has any web components to include web sites or web services, the following HTTPS requirements must be met (refer to <https://https.cio.gov/>) :

- A.** A certificate that meets the guidance below:
  - Publicly validated TLS certificates, either from HHS or a public vendor for publicly facing websites. Internal sites are allowed to use HHS certificates. Self-signed certificates are prohibited from use.
  - TLS certificate uses SHA2 as a signature algorithm.
  - TLS certificate key length of at least 2048 bits.
  - Use of wildcards is strongly discouraged.
- B.** HTTPS Only: Only HTTPS shall be utilized for all websites and web services. The use of HTTP is prohibited.
- C.** Mixed Content: All content shall be served and referenced over HTTPS. Linking to libraries, CSS, JS, fonts, iframes, etc. that load content not hosted on the server shall be served over HTTPS.
- D.** HTTP Strict Transport Security (HSTS): HSTS shall be enabled for any and all System web servers.
- E.** Perfect Forward Secrecy shall be enabled on all web servers.
- F.** The use of weak or deprecated ciphers shall not be used.
- G.** The NIH shall perform a web application vulnerability scan of any websites using the IBM AppScan commercial product. The vendor is responsible for remediating any vulnerabilities identified within the following timeframe:
  - HIGH and CRITICAL Vulnerabilities: 30 days
  - Medium Vulnerabilities: 45 days
  - LOW Vulnerabilities: 60 days.
- H.** The System shall ensure that the web site and servers are not vulnerable to the risks identified in the Open Web Application Security Project (OWASP) Top 10 list of web vulnerabilities (refer to [www.owasp.org](http://www.owasp.org)).

**PART 6 – PROJECT MANAGEMENT, IMPLEMENTATION, SERVICE**

**6.1 PROJECT MANAGEMENT**

- 6.1.1 The Contractor shall identify each key personnel to be assigned to this contract and a detailed resume shall be submitted for each key person proposed. The following personnel are considered key personnel by the government: Contract Manager, Contractor Project Manager, and Pharmacist consultant.
- 6.1.2 The Contractor shall identify all prime and subcontractor(s), management and implementation personnel to be assigned to this project and describe their credentials, roles, responsibilities, and relationships to the contract and its implementation
- 6.1.3 The Contractor shall use Microsoft Project or similar tools for providing a project plan to the NIH CC COR throughout the project deployment and across each task.
- 6.1.4 The Contractor shall provide a detailed draft plan with the proposal. (see technical questionnaire and exhibit table 1) The plan shall establish the budget, resource needs, major tasks and schedule for implementation required in accordance with American National Standards Institute/Electronic Industries Alliance (ANSI/EIA) Standard 748-A, Earned Value Management Standards, May 1998. The NIH CC and the Contractor will finalize the details such as specific dates and resources after award. The NIH CC and the Contractor will maintain the plan throughout the duration of the implementation work with regular updates provided by the Contractor.
- 6.1.5 The Contractor shall follow project management and project change management as part of the project implementation.
- 6.1.6 The Contractor shall submit the deliverables based on the content and timeframe identified under Technical Exhibit 1 – Deliverables Schedule.
- 6.1.7 The Contractor shall validate the Technical Exhibit 2 – Estimated Workload Data as part of the proposal.

**6.2 TRAINING**

- 6.2.1 The Contractor shall provide a Training Plan that encompasses all requirements proposed in the SOW. The plan shall be submitted with the Contractor proposal for consideration when making an award. Acceptance of training completion will be performed by the COR. Training is complete when the NIH CC Staff are capable and competent to independently perform all required work specific to their role using the system.
- 6.2.2 Schedule for training sessions shall be coordinated with the COR.
- 6.2.3 The Contractor shall train all staff members on the use of the system.
- 6.2.4 The Contractor shall provide at least four (5) training sessions.
- 6.2.5 The Contractor shall provide training that will include a period of live demonstration and observation of the staff using the system in each training session
- 6.2.6 The Contractor shall provide training materials to include quick reference guide(s) in addition to full documentation describing installation, support and troubleshooting steps.
- 6.2.7 The Contractor shall schedule on-site or virtual training prior to installation to be completed within two (2) weeks prior to installing the first robot.
- 6.2.8 The Contractor shall provide training agendas, schedules, presentations, manuals and reference guides to the NIH CC COR prior to conducting any training.
- 6.2.9 The Contractor shall provide electronic training materials (e.g., CD-ROM, LMS and/or ongoing access to role specific computer based training) which shall also be accessible by staff unavailable

**SOW: Autonomous Mobile Delivery Robot**

to attend in person training, staff in need of refresher training or staff who are hired after the Contractor led initial training sessions.

**6.3 SERVICE LEVEL MANAGEMENT AND SUPPORT SYSTEMS**

- 6.3.1 The Contractor shall provide service management including routine and emergent service. The NIH CC COR will determine the need for service and evaluate emergent and urgent conditions.
- 6.3.2 All repairs must meet equipment manufacturers' specifications.
- 6.3.3 The Contractor shall provide manufacturer trained staff and train certified CC employees as factory trained technicians to be first responders for unscheduled service calls.
- 6.3.4 The Contractor shall supply all parts and labor required to resolve issues. No refurbished equipment will be accepted. In the event that only a refurbished device is available the Contract Manager must notify and gain approval by the NIH CC COR.
- 6.3.5 The Contractor shall replace devices with new devices if the existing device is found defective, broken or after two (2) events were called regarding the device within one week. No refurbished equipment will be accepted. In the event that only a refurbished device is available the Contract Manager must notify and gain approval by the NIH CC COR.
- 6.3.6 The Contractor will certify monthly OS Security Updates to all MS Window Server and System Devices as needed.
- 6.3.7 The Contractor shall have an on-site response time based on the table below or provide response time and accepted by COR prior to implementation:

<b>Problem Severity</b>	<b>Respond to Call</b>	<b>Fix Problem Remotely</b>	<b>On Site Problem Resolution</b>
Warranty Issue related to component	1 hour	Within 2 hours of problem determination	Resolve issue within 4 hours of problem determination.
Production System Problem – patient safety at risk, one or more unit down, production system down or major portions unusable	1 hour	Within 2 hours of problem determination	Resolve issue within 4 hours of problem determination.
Production System Problem – major portions of system usable and mission critical workload can continue	1 hour	Within 4 hours of problem determination	Determine plan within 6 hours. Resolve issue within 8 hours of problem determination.
Production System Problem – system usable with manual workaround	1 hours	Within 12 hours of problem determination	Determine plan within 6 hours. Resolve issue within 12 hours of problem determination.
Total System Down	1 hours	Within 12 hours of problem determination	Determine plan within 4 hours. Resolve issue within 12 hours of problem determination.
Non-production System Problem	4 hours	Within 24 hours of maintenance call	Within 48 hours of maintenance call.

**6.4 HARDWARE INSTALLATION AND TESTING**

**SOW: Autonomous Mobile Delivery Robot**

- 6.4.1 Acceptance and integration testing for all components shall be completed and accepted by NIH prior to deployment.
- 6.4.2 Software Acceptance Testing - Installation of application software and third party tools designed for System Administration and Data Analytics must be completed and accepted by NIH prior to the activation.
- 6.4.3 System Readiness Testing – System readiness testing includes detailed test plans for unit and integration testing for all proposed applications and system management tools for each defined phase. The Test Plan shall include installation, certification for use, acceptance testing and ready for go-live tests for functional and infrastructure requirements. Operational test shall include performance testing for throughput, response time, reliability and security. The Test Plan shall include methodology to provide the results of all testing done under this procurement in a format acceptable to the NIH CC COR. Testing must be completed and accepted by NIH after Delivery Acceptance and prior to end user training by Unit. (See Technical Exhibit 1)

**6.5 SYSTEM ACCEPTANCE**

- 6.5.1 The Contractor will work with the NIH CC COR for acceptance of the System.
- 6.5.2 The Contractor will provide that each component will have a 15 day system acceptance period following go live.
- 6.5.3 The Contractor will work with the NIH CC COR for acceptance of Individual Components.

**6.6 WARRANTY**

- 6.6.1 The Contractor shall warrant all non-system parts, labor and installation for a desired period of one (1) year effective upon task acceptance.
- 6.6.2 The Contractor shall provide manufacturer five (5) year warranty for the robot Management parts effective upon acceptance.
- 6.6.3 The Contractor shall provide the warranty which shall include all necessary software upgrades to keep the system fully operational while in use.

**6.7 SYSTEM RETIREMENT**

- 6.7.1 The Contractor shall provide a mechanism to export data from all components in which data exists to the government with the understanding that the governments owns all data entered into the system.
- 6.7.2 The Contractor shall provide a data dictionary to understand the data being provided to the government.
- 6.7.3 The Contractor shall provide a way for the government to easily view the data in the event of system retirement.

**SOW: Autonomous Mobile Delivery Robot**

**PART 7 - APPLICABLE PUBLICATIONS**

**APPLICABLE PUBLICATIONS (CURRENT EDITIONS)** The Contractor must abide by all applicable regulations, publications, manuals, and local policies and procedures. The Contractor must provide components, material and labor that meet all applicable regulatory requirements for a hospital autonomous System, including:

- Electrical Components, Devices, and Accessories: Listed and labeled according to UL1069 as defined in NFPA 70, Article 100, by a testing agency acceptable to authorities having jurisdiction, and marked for intended use.
- Comply with NEC as applicable to construction and installation of system components and wiring.
- Conform to NFPA 70.
- Conform to HIPAA regulations relating to all patient communications including but not limited to text messaging, paging and public address systems.

**REFERENCES**

- Comprehensive Accreditation Manual for Hospitals ( [www.jointcommission.org](http://www.jointcommission.org) )
- NFPA – National Fire Protection Association (National Electrical Code NFPA 70 and 99) (<http://www.nfpa.org/codes-and-standards>)
- ADA – Americans with Disabilities Act (<http://www.ada.gov>)
- NEMA – National Electrical Manufacturers Association – Installation Standards (<http://www.nema.org>)
- U.S. Dept. of Labor / Occupational Safety and Health Administration (<http://www.osha.gov>)
- Canadian Standards Association (<http://www.csagroup.org>)

## PART 8 - DEFINITIONS & ACRONYMS

### 8.1 DEFINITIONS:

- 8.1.1 CONTRACTOR.** A supplier or vendor awarded a contract to provide specific supplies or service to the government. The term used in this contract refers to the prime.
- 8.1.2 CONTRACTING OFFICER.** A person with authority to enter into, administer, and or terminate contracts, and make related determinations and findings on behalf of the government. Note: The only individual who can legally bind the government.
- 8.1.3 CONTRACTING OFFICER'S REPRESENTATIVE (COR).** An employee of the U.S. Government appointed by the NIH CC Contracting Officer to administer the contract. Such appointment shall be in writing and shall state the scope of authority and limitations. This individual has authority to provide technical direction to the Contractor as long as that direction is within the scope of the contract, does not constitute a change, and has no funding implications. This individual does NOT have authority to change the terms and conditions of the contract.
- 8.1.4 DELIVERABLE.** Anything that can be physically delivered, but may include non-manufactured things such as meeting minutes or reports.
- 8.1.5** For purposes of this SOW; autonomous mobile pharmacy delivery robot solution may be interchanged with system or solution.

### 8.2 ACRONYMS:

- 8.2.1 ACRF.** The Ambulatory Care Research Facility (ACRF).
- 8.2.2 CRC.** The Mark O. Hatfield Clinical Research Center (CRC).
- 8.2.3 CRIS.** The Electronic Health Record (EHR) used at the NIH CC is known as the Clinical Research Information System.
- 8.2.4 EHR.** The Electronic Health Record (EHR).
- 8.2.5 NED.** NIH Enterprise Directory

## SOW: Autonomous Mobile Delivery Robot

## Technical Exhibit 1 – Deliverables Schedule (Upon Request by COR)

<b>Deliverable</b>	<b>Frequency</b>	<b># of Copies</b>	<b>Format</b>	<b>Submit To</b>
<b>Project Plan.</b> Include installation and testing schedule and overall project timeline. The Government desires delivery, which shall include installation, testing, initial training and removal of the legacy system, to be made within the base period of performance	Within 30 days of contract award. Updates provided weekly.	1	Electronic in MS Project, PDF or similar	NIH CC COR
<b>Weekly Installation Plan.</b> The Contractor shall develop deployment schedules one week in advance with the COR and the NIH CC Pharmacy Project Manager.	Weekly	3	Electronic in MS Project, PDF	NIH CC COR
<b>Security Plan.</b> Include review of security review of all aspects of the system	Within 30 days of contract award. Updates provided weekly.	1	Electronic in MS Project, PDF	NIH CC COR, NIH CC CIO
<b>Disaster Recovery and Business Continuity Plans.</b> Include DR and BC plans for each component of the system.	Within 30 days of installation.	1	Electronic as CAD Drawing and PDF	NIH CC COR, NIH CC CIO
<b>Architecture Diagrams.</b> To include: High level architectural drawing of overall system.	Within 30 days of installation.	1	Electronic as MS Visio	NIH CC COR, NIH CC CIO
<b>System Component Technical Information.</b> Brochures, Warranty Information, Specifications, Troubleshooting Guides for each software, hardware, HL7 interface, peripheral, component of the system.	With the Itemized Equipment list.	3	Electronic as PDF within a binder.	NIH CC COR
<b>Training Plan.</b> The contractor will provide training for multiple roles including: CC Pharmacy Project Manager, System Administrators, Super Users, and Day To Day Users. The plan must include description, agenda, format, schedule, role of trainee.	14 days prior to first roll-out.	1	Electronic as MS Word and PDF	NIH CC COR
<b>Quality Control Plan.</b> The contractor shall develop and maintain an effective quality control program to ensure services are performed in accordance with this PWS. The contractor shall develop and implement procedures to identify, prevent, and ensure non-recurrence of defective services.	The QCP is to be delivered with the contractors proposal if it is an evaluation factor, three copies of a comprehensive written QCP shall be submitted within 5 working days when changes are made thereafter.	1	Electronic in MS Word	NIH CC CO and NIH CC COR
<b>Quality Assurance Plan.</b> The government shall evaluate the contractor's performance under this contract in accordance with the Quality Assurance Surveillance Plan. This plan is primarily focused on what the Government must do to ensure that the contractor has performed in accordance with the performance standards. It defines how the performance standards will be applied, the frequency of surveillance, and the minimum acceptable defect rate(s).	The QASP is to be delivered with the contractor proposal. Three copies of a comprehensive written QAP shall be submitted within 5 working days when changes are made thereafter.	1	Electronic in MS Word	NIH CC CO and NIH CC COR

## SOW: Autonomous Mobile Delivery Robot

## Technical Exhibit 2 – Estimated Workload Data (Upon Request by COR)

ITEM	NAME	PROPOSE ESTIMATED QUANTITY INCLUDING HOURS	
1	<b>Contract Manager.</b> The contractor shall provide a contract manager who shall be responsible for the performance of the work. The name of this person, and an alternate who shall act for the contractor when the manager is absent, shall be designated in writing to the NIH CC Contracting Officer. The contract manager or alternate shall have full authority to act for the contractor on all contract matters relating to daily operation of this contract.		
2	<b>System Engineer.</b> The System Engineer is the technical architect, designer and engineer in charge of the overall design of the system.		
3	<b>System Installer.</b> The System Installer is responsible for all device set-up and configuration.		
4	<b>Pharmacy Consultant.</b> The pharmacy consultant shall be a pharmacist that will be available to the pharmacy informatics team during go-live and post go-live to assist with clinically related issues or problems.		
5	<b>Trainers.</b> Trainers are responsible for training all components of the system.		
6	<b>Certified Support Technicians.</b> Certified Support Technicians are responsible for servicing the system, system support, system repair and coordination of repair that he/she cannot complete.		

**Technical Exhibit 3 – CC Data Center**

- 3,000 square foot facility
- Provides redundant UPS power and redundant cooling with dedicated emergency generator power backup
- Physically secured with 24x7 staff
- Standard 24" racks for equipment with redundant 208VAC power supplied via C13 and C19 receptacles
- Systems managed by DCRI
  - Up to 10GB network connectivity
  - DCRI has dedicated groups for management of hardware, OS/patching, database and backup
  - Servers must adhere to all NIH security policies
  - Customer manages application (unless customer and DCRI have an alternate agreement)
  - Fiber connectivity to CIT core network is supplied
- Systems managed by Vendor
  - Servers must adhere to all NIH security policies
  - Remote access must follow description in Technical Exhibit 12

**SOW: Autonomous Mobile Delivery Robot**

**Technical Exhibit 4 – CC Remote Access Options**

The CC allows for several secure mechanisms that comply with NIH security and privacy policies and standards in which employees, contractors, and personnel may access CC systems remotely. The CC Security Team will work with the vendor to determine potential options; however, a potential option is stated below.

**Non-Persistent Remote Access (e.g. GoToMeeting, Secure Link, LogMeIn, VSuite, Webex, etc.)**

This option is for ad-hoc or as needed communications that may be needed within NIH or between NIH and external parties.

**Requirements:**

- CC staff must initiate the connection with external party, monitor activities, retain a log of external party's name, date/time and purpose of the connection and terminate the connection when activities are completed each time
- Must complete MOU with CC security team and Maintenance Contract
- PIV or NIH AD account is not required
- If other party is not HIPAA compliant, users must complete Secure Remote Computers training as well as the Security & Privacy Training (and Annual Refreshers) and provide evidence of completion (from NIH Public Site)
- If other party is HIPAA compliant, must show evidence of relevant training
- If Remote Access is needed only for a short term (6 months or less), no MOU is needed; For long term use, MOU will be needed